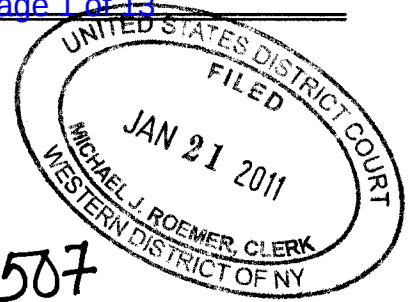


# UNITED STATES DISTRICT COURT

for the  
Western District of New York



In the Matter of the Search of  
(Briefly describe the property to be searched or identify the person by name and address.)  
AMCHAR WHOLESALE, INC. and AMERICAN  
TACTICAL IMPORTS, INC., 100 Airpark Drive,  
Rochester, New York

Case No. 11-MJ-507

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Western District of New York  
(identify the person or describe property to be searched and give its location):

The subject premises to be search is 100 Airpark Drive, Rochester, NY, more particularly described in Attachment A.

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

See attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ more fully described in the attached Affidavit in Support of Search and Seizure Warrant;
- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of 18 U.S.C. §§ 545 and 542, and the application is based on these facts which are continued on the attached sheet..

☐ Delayed notice of      days (give exact ending date if more than 30 days:                     ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

*Mark T. Haggerty*

Applicant's signature

MARK HAGGERTY, Special Agent  
U.S. Department of Homeland Security

Printed name and title

Sworn to before me and signed in my presence.

Date: January 21, 2011

*Jonathan W. Feldman*

Judge's signature

City and state: Rochester, NY

Honorable Jonathan W. Feldman, U.S. Magistrate Judge

Printed name and title

11 mj 507

**Attachment A****The Premises to be Searched**

The location known as **100 Airpark Drive, Rochester, NY 14624**, can be further described as a two (2) story structure that faces Scottsville Road (Route 383). The structure has light blue concrete façade on the first story of the front of the building (facing Scottsville Road). The concrete façade continues for a small portion on the left side of the structure. The remaining material of the structure consists of white corrugated steel. There is one (1) bay garage door and two (2) loading docks located on the left side of the structure. There is a fairly large parking lot to the left of the structure. The name of "AMCHAR" is visibly displayed with red lettering on the front of the structure, with a blue door toward the right front of the structure. There are several thin vertical windows located on the first and second story on the front of the structure, as well as some on the left side of the structure. The number "100" is affixed to the north side of the building above a blue awning, which serves as the main entrance to the structure.

**Attachment B**

**The Items to be Seized**

The following items to be seized at the location to be searched listed in **Attachment A**, including items, records, documents, materials and files, whether in physical, documentary, or electronic form, to include:

1. Any and all business records, as well as communications, whether in electronic or hard copy form, in the possession of ANTHONY DICHARIO, AMCHAR WHOLESALE, INC. and AMERICAN TACTICAL IMPORTS, Inc., and CHRIS MARZAHN relating to Karl Kleber and/or TRANSARMS HANDELSGESELLSCHAFT, MBH and Co. KG and the sale, purchase and/or importation of firearms and component parts and ammunition, and relating to the importation of AK 47 parts kits manufactured in China, among other places, by **AMCHAR WHOLESALE, INC.** and **AMERICAN TACTICAL IMPORTS, INC.**, as well as actual firearms and component parts and ammunition, which are evidence of and fruits or instrumentalities of violations of Title 18, United States Code, Section 545 and 542, and any mechanism used for the receipt, storage, or transmission of items in furtherance of the same, including:

- a. All of the above-described documentation and records stored on/in computer floppy disks, thumb devices, CD's, tape media, or other electronic media that may contain copies of computer programs and/or files.
- b. Any computer, computer hardware, computer system and related peripherals, including but not limited to any data processing devices and software (such as central processing units, memory typewriters, and self-contained "laptop" or

“notebook” computers), internal and peripheral storage devices (such as fixed disks, external hard drives, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, transistor-like binary devices, routers, computer compact disks, CD-ROMS, DVD, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printers, video display monitors, scanners, optical readers, digital cameras, and related communications devices such as cables and connections); related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices and electronic tone-generating devices); cellular telephones; as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

- c. Computer passwords, counter-forensic programs and other data security devices designated to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alphanumeric characters) usually operates as a sort of digital key to “unlock” particular data security devices, chips, and circuit boards. Data security software or digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software may also encrypt, compress, hide or “booby-trap” protected data to make it inaccessible or unusual, as well as reverse the process to restore it.
- d. Any and all documents, records, images, videos, emails, email software, associated email addresses, email address book contents, internet history, browsing history, internet search history, cookies, deleted files, bookmarked and favorite web pages, user typed web addresses, desktop shortcuts, path and file names for files opened through any media and/or image viewing software, chat software, chat files, chat logs, chat names used, peer to peer software, peer to peer files, newsgroup postings by the user, IP addresses assigned, and other evidence pertaining to the receipt, distribution, transmission, advertisement, and possession as it relates to smuggling goods into the United States and Entry of Goods by Means of False Statements;

- e. Computer software stored in electronic, magnetic, optical or other digital form. Including programs to run operating systems, application (like word processing, graphics or spreadsheet programs), utilities, interpreters, and communications programs.
- f. Any and all records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment found in the business.
- g. Computer-related documentation consisting of written, recorded, printed or electronically stored material, which explains or illustrates how to configure or use computer hardware, software, or other related items.
- h. Documents and records regarding the ownership, usage and/or possession of the searched premises.
- i. Photographs: Entry and exit photographs of the premises to be searched, as well as photographs of the specific places in which items are found and from which items are seized.

**SUPPLEMENTAL AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT**

STATE OF NEW YORK     )  
COUNTY OF MONROE    )     SS:  
CITY OF ROCHESTER     )

I, Mark Haggerty, being duly sworn, depose and state the following:

1) I am a Special Agent with United States Homeland Security Investigations (hereinafter referred to as HSI) and its predecessor United States Immigration and Customs Enforcement (ICE), and have been so employed for approximately two and one half (2 ½) years. As a part of my duties as a Special Agent with HSI and formerly ICE, I investigate crimes involving counter proliferation, violations of export control laws and other customs violations.

2. This affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the business(es) of **AMCHAR WHOLESALE, INC.** and **AMERICAN TACTICAL IMPORTS, INC.**, two (2) interrelated companies, all of which are located at 100 Airpark Drive, Rochester, New York, hereinafter, "PREMISES," further described in Attachment A, for certain items, particularly described in Attachment B.

3. On January 13, 2011, this Court issued a search warrant, bearing Miscellaneous Criminal Number 11-MJ-503, authorizing the search of the subject PREMISES and seizure of certain evidence, fruits, and instrumentalities, based upon the application and affidavit attached hereto as Exhibit 1, the allegations of which are incorporated by reference as if fully set forth

herein. As a result of additional information obtained subsequent to this Court issuance of that search warrant, bearing Miscellaneous Criminal Number 11-MJ-503, a decision was made not to execute that search warrant but, instead, to seek a new search warrant authorizing the seizure of additional evidence, fruits and instrumentalities.

4. Subsequent to the Court authorizing the search warrant bearing Miscellaneous Criminal Number 11-MJ-503, your affiant has spoken with a confidential source (hereinafter CS-1), whose name is being withheld to protect his/her identity. CS-1, who had previously been arrested and charged with violation of federal criminal law, as part of a subsequent debriefing conducted pursuant to a proffer agreement between CS-1 and the government, made admissions which were contrary to his own penal interests regarding CS-1's role in the unlawful importation of Chinese AK-47 gun magazines into the United States through **ANTHONY DICHARIO, AMCHAR WHOLESALE, INC.** and **AMERICAN TACTICAL IMPORTS, INC.** In addition, CS-1 indicated that within the past few month, CS-1 exchanged emails with a person named Chris Marzahn (Marzahn), an import manager and employee of **AMCHAR WHOLESALE, INC.** and **AMERICAN TACTICAL IMPORTS, INC.** During that email exchange, CS-1 indicated that CS-1 would be able to provide **AMCHAR WHOLESALE, INC.** and **AMERICAN TACTICAL IMPORTS, INC.** with AK 47 parts kits which CS-1 told Marzahn were manufactured in China, Russia and Serbia. As such, both CS-1 and Mazahn knew that those AK 47 parts kits could not be legally imported into the United States. According to CS-1, Marzahn said that **AMCHAR WHOLESALE, INC.** and **AMERICAN TACTICAL IMPORTS, INC.** was interested in pursuing the deal further even after being informed of the countries of origin.

5. Subsequent investigation has confirmed that CS-1 is known to Marzahn and has responded to a communication inquiring about the AK 47 parts deal from CS-1. The response did not specifically address the importation of AK 47 parts kits, but in it Marzahn did express a desire to continue to deal with CS-1.

6. Based on the foregoing as well as the copy of the search warrant and affidavit in support of a search warrant to search the PREMISES signed by the Court on January 13, 2011, a copy of which is attached and incorporated as Exhibit 1, there is probable cause to believe that the PREMISES also contains information showing contact between **AMCHAR WHOLESALE, INC.** and **AMERICAN TACTICAL IMPORTS, INC.**, its principals and Chris Marzahn and Karl KLEBER and other individuals relating to the importation of AK 47 parts kits manufactured in China and Russia by **AMCHAR WHOLESALE, INC.** and **AMERICAN TACTICAL IMPORTS, INC.**

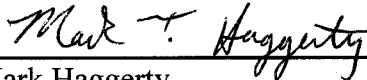
7. Based on the foregoing as well as the copy of the search warrant and affidavit in support of a search warrant to search the PREMISES signed by the Court on January 13, 2011, a copy of which is attached and incorporated as Exhibit 1, there is probable cause to believe that at **100 Airpark Drive, Rochester, New York 14624**, which is more fully described and pictured in **Attachment A**, there is located evidence, fruits and/or instrumentalities of the violations specified in this affidavit, as well specified in Exhibit 1.



8. Based on the foregoing as well as the copy of the search warrant and affidavit in support of a search warrant to search the PREMISES signed by the Court on January 13, 2011, a copy of which is attached and incorporated as Exhibit 1, there is probable cause to believe the items set out in **Attachment B** will be located at the above location, whether such items are stored in physical, documentary, or electronic form.

**CONCLUSION**

9. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in **Attachment A** and seize the items described in **Attachment B**.

  
\_\_\_\_\_  
Mark Haggerty  
Special Agent  
Immigration & Customs Enforcement  
Homeland Security Investigations

Sworn to and subscribed  
before me this 21 day of  
January 2011.

  
\_\_\_\_\_  
HONORABLE JONATHAN W. FELDMAN  
UNITED STATES MAGISTRATE JUDGE

**Attachment A**

**The Premises to be Searched**

The location known as **100 Airpark Drive, Rochester, NY 14624**, can be further described as a two (2) story structure that faces Scottsville Road (Route 383). The structure has light blue concrete façade on the first story of the front of the building (facing Scottsville Road). The concrete façade continues for a small portion on the left side of the structure. The remaining material of the structure consists of white corrugated steel. There is one (1) bay garage door and two (2) loading docks located on the left side of the structure. There is a fairly large parking lot to the left of the structure. The name of "AMCHAR" is visibly displayed with red lettering on the front of the structure, with a blue door toward the right front of the structure. There are several thin vertical windows located on the first and second story on the front of the structure, as well as some on the left side of the structure. The number "100" is affixed to the north side of the building above a blue awning, which serves as the main entrance to the structure.

**Attachment B**

**The Items to be Seized**

The following items to be seized at the location to be searched listed in **Attachment A**, including items, records, documents, materials and files, whether in physical, documentary, or electronic form, to include:

1. Any and all business records, as well as communications, whether in electronic or hard copy form, in the possession of ANTHONY DICHARIO, AMCHAR WHOLESALE, INC. and AMERICAN TACTICAL IMPORTS, Inc., and CHRIS MARZAHN relating to Karl Kleber and/or TRANSARMS HANDELSGESELLSCHAFT, MBH and Co. KG and the sale, purchase and/or importation of firearms and component parts and ammunition, and relating to the importation of AK 47 parts kits manufactured in China, among other <sup>prohibited parts</sup> places, by **AMCHAR WHOLESALE, INC.** and **AMERICAN TACTICAL IMPORTS, INC.**, as well as actual firearms and component parts and ammunition, which are evidence of and fruits or instrumentalities of violations of Title 18, United States Code, Section 545 and 542, and any mechanism used for the receipt, storage, or transmission of items in furtherance of the same, including:

- a. All of the above-described documentation and records stored on/in computer floppy disks, thumb devices, CD's, tape media, or other electronic media that may contain copies of computer programs and/or files.
- b. Any computer, computer hardware, computer system and related peripherals, including but not limited to any data processing devices and software (such as central processing units, memory typewriters, and self-contained "laptop" or

“notebook” computers), internal and peripheral storage devices (such as fixed disks, external hard drives, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, transistor-like binary devices, routers, computer compact disks, CD-ROMS, DVD, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printers, video display monitors, scanners, optical readers, digital cameras, and related communications devices such as cables and connections); related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices and electronic tone-generating devices); cellular telephones; as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

- c. Computer passwords, counter-forensic programs and other data security devices designated to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alphanumeric characters) usually operates as a sort of digital key to “unlock” particular data security devices, chips, and circuit boards. Data security software or digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software may also encrypt, compress, hide or “booby-trap” protected data to make it inaccessible or unusual, as well as reverse the process to restore it.
- d. Any and all documents, records, images, videos, emails, email software, associated email addresses, email address book contents, internet history, browsing history, internet search history, cookies, deleted files, bookmarked and favorite web pages, user typed web addresses, desktop shortcuts, path and file names for files opened through any media and/or image viewing software, chat software, chat files, chat logs, chat names used, peer to peer software, peer to peer files, newsgroup postings by the user, IP addresses assigned, and other evidence pertaining to the receipt, distribution, transmission, advertisement, and possession as it relates to smuggling goods into the United States and Entry of Goods by Means of False Statements;

- e. Computer software stored in electronic, magnetic, optical or other digital form. Including programs to run operating systems, application (like word processing, graphics or spreadsheet programs), utilities, interpreters, and communications programs.
- f. Any and all records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment found in the business.
- g. Computer-related documentation consisting of written, recorded, printed or electronically stored material, which explains or illustrates how to configure or use computer hardware, software, or other related items.
- h. Documents and records regarding the ownership, usage and/or possession of the searched premises.
- i. Photographs: Entry and exit photographs of the premises to be searched, as well as photographs of the specific places in which items are found and from which items are seized.